Claims

What is claimed is:

1. A method of communicating private data between computers coupled to a data communication network, said method comprising:

receiving, at a network server, private data encrypted by a first client as a function of a wrapping key unknown to the server, said server and said first client being coupled to the data communication network;

storing the received encrypted private data at the server;

receiving, at the server, a request from a second client for the encrypted private data; and

in response to the received request, transferring the encrypted private data from the server to the second client for decryption as a function of the wrapping key.

2. The method of claim 1, wherein receiving the encrypted private data includes receiving an encrypted private key, said encrypted private key being representative of a private key associated with the first client and encrypted as a function of the wrapping key, said wrapping key being generated on the first client in response to an encryption password received from a user of the first client.

3. The method of claim 2, further comprising decrypting the encrypted private key at the second client as a function of the wrapping key, said wrapping key being generated on the second client in response to the encryption password received from a user of the second client.

4. The method of claim 2, further comprising:

receiving, at the server, the wrapping key encrypted by the first client as a function of a recovery key unknown to the server, said recovery key being generated on the first client in response to a recovery option selected by the user; and

receiving, at the server, the recovery key encrypted by the first client as a function of the wrapping key.

5. The method of claim 4, further comprising:

generating, at the server, a backup key in response to encrypted private data received from the first client;

storing the generated backup key in a database associated with the server;

retrieving the stored backup key in response to a recovery request received from the user of the first client; and

transferring the backup key from the server to the first client via the data communication network in response to the received recovery request, said first client generating a backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key for storage on the first client, said backup key being known to the server.

6. The method of claim 5, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the first client in response to the received recovery request, said backup encrypted recovery key stored on the first client being decrypted, at the first client, as a function of the transferred backup key to obtain the recovery key, said encrypted wrapping key being decrypted, at the first client, as a function of the obtained recovery key to obtain the wrapping key, and said encrypted private key being decrypted, at the first client, as a function of the obtained wrapping key to obtain the private key.

7. The method of claim 5, further comprising transferring the encrypted recovery key and the transferred backup key to the second client in response to a backup request received from the user of the second client, said transferred encrypted recovery key being decrypted, at the second client, as a function of the wrapping key generated on the second client to obtain the recovery key, said second client encrypting the obtained recovery key as a function of the transferred backup key to generate the backup encrypted recovery key for storage in a memory associated with the second client.

8. The method of claim 5, further comprising:

retrieving the stored backup key from the database associated with the server in response to a recovery request received from the user of the second client; and

transferring the backup key from the server to the second client in response to the received recovery request.

9. The method of claim 5, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the second client in response to a recovery request received from the second client via the data communication network, said backup encrypted recovery key stored on the second client being decrypted, at the second client, as a function of the transferred backup key to obtain the recovery key, said encrypted wrapping key being decrypted, at the second client, as a function of the obtained recovery key, and said encrypted private key being decrypted, at the second client, as a function of the obtained wrapping key to obtain the private key.

10. The method of claim 1 wherein the second client is a roaming client computer coupled to the data communication network.

11. One or more computer readable media having computer-executable instructions for performing the method of claim 1.

12. A system for communicating private data on a data communication network, comprising:

a server receiving private data encrypted by a first client as a function of a wrapping key unknown to the server, said server and said first client being coupled to the data communication network;

a database associated with the server, said server being configured to store the received encrypted private data in the database and to transfer the stored encrypted private data to a second client also coupled to the data communication network for decryption as a function of a wrapping key in response to a request for the encrypted private data received from the second client.

13. The system of claim 12, wherein the encrypted private data comprises a private key associated with the first client and encrypted as a function of the wrapping key, said wrapping key being generated on the first client responsive to an encryption password received from a user of the first client.

14. The system of claim 13, wherein the first client is configured to generate the wrapping key on the first client, encrypt the private data as a function of the generated wrapping key, and generate a recovery key for storage on the first client.

15. The system of claim 13, wherein the second client is configured to generate the wrapping key on the second client computer and decrypt the transferred encrypted private data as a function of the wrapping key generated on the second client, and wherein said wrapping key is generated on the second client computer in response to the encryption password received from a user of the second client.

16. The system of claim 15, further comprising computer-readable instructions implementing a server application and wherein the server is responsive to a storage request received from the user of the first client computer to execute the server application for storing the received encrypted data in the database, generating a backup key for storage in the database, and transferring the generated backup key to the first client computer, said backup key being used by the first client computer to generate a second encrypted recovery key for storage on the first client computer.

17. The system of claim 16 wherein the backup key is randomly generated by the server in response to receiving encrypted private data from the first client.

18. The system of claim 17 wherein the received encrypted private data includes an encrypted private key representative of a private key associated with the first client encrypted as a function of the wrapping key, an encrypted wrapping key representative of the wrapping key encrypted as a function of the recovery key, and a first encrypted

recovery key representative of the recovery key encrypted as a function of the wrapping key.

19. The system of claim 18 wherein the server is further configured to transfer the first encrypted recovery key and the backup key to the second client in response to a backup request received from the second client, said backup request including the defined backup password, said transferred first encrypted recovery key being decrypted at the second client as a function of the wrapping key generated on the second client computer to obtain the recovery key, said obtained recovery key being encrypted as a function of the transferred backup key to generate the second encrypted recovery key for storage in a memory associated with the second client computer.

20. The system of claim 19 wherein the server is further configured to transfer the encrypted private key, the generated backup key, and the encrypted wrapping key to the second client computer in response to a recovery request received from the second client computer, wherein the second encrypted recovery key stored in the memory associated with the second client computer is decrypted, at the second client, as a function of the transferred backup key to obtain the recovery key, said transferred encrypted wrapping key being decrypted, at the second client, as a function of the obtained recovery key to obtain the wrapping key, said transferred encrypted private key being decrypted, at the second client, as a function of the obtained wrapping key to obtain the private key.

21. A computer readable medium comprising computer-executable instructions for communicating private data between computers coupled to a data communication network, said computer-readable medium comprising:

first receiving instructions for receiving, at a network server, private data encrypted by a first client as a function of a wrapping key unknown to the server, said server and said first client being coupled to the data communication network;

storing instructions for storing the received encrypted private data at the server;

second receiving instructions for receiving, at the server, a request from a second client for the encrypted private data; and

transferring instructions for transferring the encrypted private data from the server to the second client for decryption as a function of the wrapping key in response to the received request.

22. The computer readable medium of claim 21, wherein the first receiving instructions include instruction for receiving an encrypted private key ($E_{K1}PK$) representative of a private key, associated with the first client, encrypted as a function of the wrapping key , said wrapping key being generated on the first client responsive to an encryption password received from a user of the first client.

23. The computer readable medium of claim 22, wherein the transferring instruction includes instruction for transferring the encrypted private key, said encrypted private key being decrypted, at the second client, as a function of the wrapping key, said wrapping key being generated on the second client responsive to the encryption password received from a user of the second client.

24. The computer readable medium of claim 22 wherein the first receiving instructions further include instructions for receiving, at the server, the wrapping key encrypted by the first client as a function of a recovery key unknown to the server, said recovery key being generated on the first client in response to a recovery option selected by the user via the first client, and receiving, at the server, the recovery key encrypted by the first client as a function of the wrapping key.

25. A method of communicating private data between computers coupled to a data communication network, said method comprising:

receiving, at a server, a request from a roaming client for encrypted private data, said request including a digest or hashed value of an authentication password, said server and said roaming client being coupled to the data communication network;

determining if a form of the authentication password received from the roaming client is valid;

retrieving, when a form of the authentication password is valid, the encrypted private data, said private data being previously encrypted as a function of an encryption password unknown to the server;

transferring the retrieved encrypted private data from the server to the roaming client for decryption as a function of the wrapping key.

26. The method of claim 25, wherein retrieving the encrypted private data includes retrieving an encrypted private key, said encrypted private key being representative of a private key associated with the home client and encrypted as a function of the wrapping key, said wrapping key being generated on the home client in response to an encryption password received from a user of the home client.

27. The method of claim 26, further comprising decrypting the transferred encrypted private key at the roaming client as a function of the wrapping key, said wrapping key being generated on the roaming client in response to the encryption password received from a user of the roaming client.

28. The method of claim 27, further comprising:

retrieving the wrapping key encrypted by the home client as a function of a recovery key unknown to the server, said recovery key being generated on the home client in response recovery option selected by the user via the home client;

retrieving the recovery key encrypted by the home client as a function of the wrapping key;

decrypting, at the roaming client, the encrypted recovery key as a function of the wrapping key generated on the roaming client to obtain the recovery key ;

retrieving a stored backup key in response to a backup request received from the user of the roaming client, said backup key generated at the server in response to receiving encrypted private data from the home client;

transferring the backup key from the server to the roaming client via the data communication network in a secure manner in response to the received recovery request,

said roaming client encrypting the obtained recovery key as a function of the retreived backup key; and

storing, on the roaming client, a backup encrypted recovery key representative of the recovery key encrypted as a function of the transferred backup key.

29. The method of claim 28, further comprising:

retrieving the stored backup key in response to a recovery request received from the user of the roaming client, said backup key generated at the server in response to receiving encrypted private data from the home client;

transferring the backup key from the server to the roaming client via the data communication network in a secure manner in response to the received recovery request, said roaming client decrypting the backup encrypted recovery key to obtain the recovery key.

30. The method of claim 29, further comprising transferring the encrypted private key and the encrypted wrapping key from the server to the roaming client in response to the received recovery request, said encrypted wrapping key being decrypted, at the roaming client, as a function of the obtained recovery key to obtain the wrapping key, and said encrypted private key being decrypted, at the roaming client, as a function of the obtained wrapping key to obtain the private key.

31. A computer-readable medium having stored thereon a data structure, comprising:

a first data field containing private data;

a second data field containing key data representative of an input data stream received from a user; and

a third function field for encrypting the private data as a function of the key data, and for transferring the encrypted private data to a central location for storage.

32. The computer readable medium of claim 31, wherein the encrypted private data includes an encrypted private key, said encrypted private key being representative of a private key associated with a home client and encrypted as a function of a wrapping key,

said wrapping key being generated on the home client in response to an encryption password received from a user of the home client.